Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 26 February 2019

Case Number: T 1671/15 - 3.5.05

Application Number: 06766454.0

Publication Number: 1895399

IPC: G06F3/12, B41J29/38

Language of the proceedings: EN

Title of invention:
Printing system and program

Applicant:
Dai Nippon Printing Co., Ltd.

Headword:
Secure printing/DAI

Relevant legal provisions:
EPC Art. 56
RPBA Art. 15(3)

Keyword:
Oral proceedings held in the absence of the appellant
Inventive step - (no)

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1671/15 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 26 February 2019

Appellant: (Applicant)	Dai Nippon Printing Co., Ltd. 1-1, Ichigaya Kagacho 1-chome, Shinjuku-ku Tokyo 162-8001 (JP)
Representative:	Miller, James Lionel Woolverton Kilburn & Strode LLP Lacon London 84 Theobalds Road London WC1X 8NL (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 9 February 2015 refusing European patent application No. 06766454.0 pursuant to Article 97(2) EPC**

Composition of the Board:

Chair	A. Ritzka
Members:	K. Bengi-Akyuerek
	D. Prietzel-Funk

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division to refuse the present European patent application for lack of inventive step (Article 56 EPC) with respect to the claims of a main request and a first auxiliary request, having regard to the disclosure of

D1: US-A-2004/0049684.

Further, a second and third auxiliary request were not admitted into the examination proceedings under Rule 137(3) EPC on the grounds that they were late-filed and not clearly allowable under Article 123(2) EPC.

II. With the statement setting out the grounds of appeal, the appellant filed amended sets of claims according to a main request and first to fourth auxiliary requests. It requested that the examining division's decision be set aside and that a patent be granted on the basis of one of the above claim requests. In addition, oral proceedings were requested as an auxiliary measure.

III. In a communication annexed to the summons to oral proceedings pursuant to Article 15(1) RPBA, the board gave its preliminary opinion on the appeal. It introduced the following prior-art documents into the appeal proceedings in reaction to the appellant's arguments and newly submitted auxiliary requests:

D6: US-A-2004/0187022;
D7: US-A-2001/0038462.

In particular, the board indicated that the

subject-matter of all the claim requests on file appeared to lack inventive step (Article 56 EPC), having regard to prior-art documents D1, D6 and D7.

IV. In a letter of reply, the appellant indicated that it would not be attending the oral proceedings. It did not submit any comments on the substance of the board's communication.

V. Oral proceedings were held as scheduled on 26 February 2019 in the absence of the appellant. The board established from the file that the appellant's final requests were that the decision under appeal be set aside and that a patent be granted on the basis of the claims according to one of a main request and first to fourth auxiliary requests, all submitted with the statement setting out the grounds of appeal.

VI. Claim 1 of the **main request** reads as follows:

"A printing system (1, 1-2) comprising:

a plurality of printer apparatuses (20A, 20B, 20C) each having: printing means (28) performing printing based on print data (28); and

a print data supplying apparatus (30) for supplying print data to the plurality of printer apparatuses,

authentication information input means (24, 14) for inputting authentication information for authenticating print instruction authority of a user carrying out print instructions; and

authentication means (211, 113) for authenticating the print instruction authority of a user based on authentication information inputted by the authentication information input means,

a print attribute setting means (112) for performing setting of print attributes including

setting of a security level for the print data in accordance with user instructions,

a print data restricting means (311) for restricting the print data supplied to the printing means to within a range of the print instructing authority authenticated by the authentication means and characterised in that the print data supplying apparatus has a printer apparatus storage means (33) for storing a security level of each printing means of the plurality of printer apparatuses based on an installation environment of the printing means, and

wherein the print data restricting means (311, 213) is further for determining whether to supply the print data to the printer apparatus based on the security level for the print data and the security level of the printing means for each printer apparatus."

Claim 1 of the **first auxiliary request** reads as follows (amendments compared with claim 1 of the main request highlighted by the board):

"A printing system (1, 1-2) comprising:

a plurality of printer apparatuses (20A, 20B, 20C) each having: printing means (28) performing printing based on print data (28); ~~and~~

~~a print data supplying apparatus (30) for supplying print data to the plurality of printer apparatuses,~~

authentication information input means (24~~, 14~~) for inputting authentication information for authenticating print instruction authority of a user carrying out print instructions; and authentication means (211~~, 113~~) for authenticating the print instruction authority of a user based on authentication information inputted by the authentication information input means;

the system further comprising:

a print data supplying apparatus (30) for supplying

print data to the plurality of printer apparatuses; and

a print attribute setting means (112) for performing setting of print attributes including setting of a security level for the print data in accordance with user instructions,

a print data restricting means (311) for restricting the print data supplied to the printing means to within a range of the print instructing authority authenticated by the authentication means and characterised in that the print data supplying apparatus has a printer apparatus storage means (33) for storing a security level of each printing means of the plurality of printer apparatuses based on an installation environment of the printing means, and

wherein the print data restricting means (311, 213) is further for determining whether to supply the print data to the printer apparatus based on the security level for the print data and the security level of the printing means for each printer apparatus."

Claim 1 of the **second and third auxiliary requests** reads as follows (amendments compared with claim 1 of the first auxiliary request highlighted by the board):

"A printing system (1, 1-2) comprising:

a plurality of printer apparatuses (20A, 20B, 20C) each having: printing means (28) performing printing based on print data (28); authentication information input means (24) for inputting authentication information for authenticating print instruction authority of a user carrying out print instructions; and authentication means (211) for authenticating the print instruction authority of a user based on authentication information inputted by the authentication information input means;

the system further comprising:

a print data supplying apparatus (30) for supplying print data to the plurality of printer apparatuses; and

a print attribute setting means (112) for performing setting of print attributes including setting of a security level for the print data in accordance with user instructions,

a print data restricting means (311) for restricting the print data supplied to the printing means to within a range of the print instructing authority authenticated by the authentication means and characterised in that the print data supplying apparatus has a printer apparatus storage means (33) for ~~storing~~ recording printer apparatus management information for each of the plurality of printer apparatuses (20A, 20B, 20C) having security attributes of each of the printer apparatuses including a security level of each printing means of the plurality of printer apparatuses based on an installation environment of each of the printing means, and

wherein the print data restricting means (311, 213) is further for determining whether to supply the print data to the printer apparatus based on the security level for the print data and the security level of the printing means for each printer apparatus

wherein the printing system is configured to restrict printing the data on a printer apparatus identified by the print data restricting means when the security attributes for the print data has a security level higher than the security attributes of a printer apparatus among the printer apparatuses (20A, 20B, 20C),

wherein the print data restricting means (311) comprises data erasing means for erasing print data that has not been a target of a print instruction for at least a predetermined period, and

the printer apparatus attribute storage means (33) stores a print history information for an indication that the data erasing means carried out erasing the print data."

Claim 1 of the **fourth auxiliary request** reads as follows:

"A printing system (1, 1-2) comprising:
a plurality of printer apparatuses (20A, 20B, 20C) each having: printing means (28) performing printing based on print data (28);
authentication information input means (24) for inputting authentication information for authenticating print instruction authority of a user carrying out print instructions; and
authentication means (211) for authenticating the print instruction authority of a user based on authentication information inputted by the authentication information input means;
the system further comprising:
a print data supplying apparatus (30) for supplying print data to the plurality of printer apparatuses;
an input portion (15) for receiving print instructions from a user;
a print attribute setting means (112) for performing setting of print attributes including receiving from the input portion (15) security attributes for the print data input by the user during the input of the print instructions for instructing formation of the print data from the user and setting the security attributes for the print data;
a printer apparatus attribute storage means (33) for recording printer apparatus management information for each of the plurality of printer apparatuses (20A, 20B, 20C) having security attributes of each of the

printer apparatuses including ~~a~~ security level based on environment of each of the printer apparatuses (20A, 20B, 20C), the security level being set at each of the printer apparatuses (20A, 20B, 20C);

a print data restricting means (311) for determining whether to provide the print data to each of the printer apparatuses (20A, 20B, 20C) based on the security attributes for the print data and the security attributes based on a degree of safety of an installation environment of each of the printer apparatuses (20A, 20B, 20C), wherein a trigger for a start of a print processing occurs upon detection of availability of reading of the authentication information,

wherein the print data restricting means (311) identifies printer apparatuses (20A, 20B, 20C) that are permitted to print based on the print instruction authority authenticated by the authentication means,

wherein the printing system restricts printing the data on a printer apparatus identified by the print data restricting means when the security attributes for the print data has a security level higher than the security attributes of a printer apparatus among the printer apparatuses (20A, 20B, 20C),

wherein the print data restricting means (311) comprises data erasing means for erasing print data that has not been a target of a print instruction for at least a predetermined period, and

the printer apparatus attribute storage means (33) stores a print history information for an indication that the data erasing means carried out erasing the print data."

Reasons for the Decision

1. *Non-attendance of the appellant at oral proceedings*

1.1 The appellant decided not to attend the scheduled oral proceedings before the board (cf. point IV above). Pursuant to Article 15(3) RPBA, the board is not "obliged to delay any step in the proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned who may then be treated as relying only on its written case."

1.2 In the present case, the appellant did not respond in substance to the objections raised in the board's communication under Article 15(1) RPBA. The board re-considered the claim requests on file and maintained its objections under Article 56 EPC it had raised in its communication. So, in the exercise of its discretion under Article 15(3) RPBA, the board took a decision at the end of the oral proceedings, in the absence of the duly summoned appellant.

2. *The present invention*

The present application is concerned with a printer network system. It describes two embodiments: a *first embodiment* relating to a centralised, manager-based printer system (see page 13, line 5 to page 28, line 7; Figs. 1 to 4 of the application as filed) and a *second embodiment* relating to a distributed printer system without any manager (see page 28, line 8 to page 31, line 13 as filed). They both rely on checking whether the security level of the data to be printed matches with the security level of the printer at which the

user wants to print the respective print data before forwarding the corresponding print data to the printer.

According to the description, the object of the present invention is to avoid that a printer apparatus is utilised illegally without being noticed and thereby to improve security (see page 2, lines 13-22 as filed).

3. MAIN REQUEST

Claim 1 of the main request comprises the following limiting features, as labelled by the board:

A printing system comprising:

A) a plurality of printer apparatuses each having printing means performing printing based on print data;

B) a print data supplying apparatus for supplying print data to the plurality of printer apparatuses;

C) authentication information input means for inputting authentication information for authenticating print instruction authority of a user carrying out print instructions;

D) authentication means for authenticating the print instruction authority of a user based on authentication information inputted by the authentication information input means;

E) a print attribute setting means for performing setting of print attributes including setting of a security level for the print data in accordance with user instructions;

F) a print data restricting means for restricting the print data supplied to the printing means to within a range of the print instructing authority authenticated by the authentication means,

G) wherein the print data supplying apparatus has a printer apparatus storage means for storing a security level of each printing means of the plurality of printer apparatuses based on an installation environment of the printing means,

H) wherein the print data restricting means is further for determining whether to supply the print data to the printer apparatus based on the security level for the print data and the security level of the printing means for each printer apparatus.

3.1 *Novelty and inventive step (Articles 54 and 56 EPC)*

The board concurs with the finding of the decision under appeal that the subject-matter of present claim 1 is novel but lacks an inventive step, for the reasons set out below.

3.1.1 It is common ground that document **D1** fails to anticipate feature H) of present claim 1, i.e. that the print data restricting means is configured to determine whether to supply the print data to the printer apparatus based on the security level for the print data and the security level of the printing means for each printer apparatus (see also Grounds of Appeal, sections 2.3.2 and 2.4.5). More specifically, the system of D1 does not prevent the transmission of the data to be printed to the respective printer apparatus if the security level for the print data does not match with the security level of the printing apparatus. Thus, the subject-matter of present claim 1 is considered to be novel over D1 (Article 54 EPC).

3.1.2 As to the assessment of inventive step, the board accepts that distinguishing feature H) has the

technical effect that "print data may only be sent to a printer if the printer has the required security settings for the data in question" (see Grounds of Appeal, section 2.4.3). The board concludes that the objective technical problem to be solved may be framed as "how to prevent an authorised user from printing data on a printer which does not have the desired security requirements in the system of D1", i.e. how to avoid human errors in the printing process of D1 (see also Grounds of Appeal, section 2.4.8).

3.1.3 The board holds that the skilled person would recognise from the teaching of D1 that - besides the installation location of the printer apparatus (i.e. a printer's security level) - also the authentication level and the level of confidentiality of data to be printed (i.e. print data's security level) are taken into account as security parameters (see e.g. paragraphs [0065] to [0069] and [0072] to [0075], [0119]), and that such security data could be processed outside the printer by another unit (see e.g. paragraphs [0046] and [0085]). Therefore, the person skilled in the field of network printer systems would seek feasible ways of automatically processing that available security data at an external (e.g. central) unit in order to solve the above-identified objective problem.

To this end, the skilled person would consider e.g. prior-art document **D6**, which is also dealing with a network printer system made up of host computers, printer devices and storage devices for managing print data (see e.g. abstract and Fig. 1). The system of D6 differentiates between security levels of the print data ("high/top secret"; "medium"; "low") and the security levels of the individual printers ("top secret"; "high"; "medium"; "low") through respective

lists (see e.g. Figs. 3(a) and 3(b)). Moreover, D6 clearly teaches that the data to be printed is only transmitted to the corresponding printer apparatus if the security levels of that printer and the print data match, in full accordance with feature H) of present claim 1 (see e.g. D6, paragraphs [0164] to [0167]: *"If the user selects a storage containing target print data ... it is determined ... whether the desired print data stored in the storage is suitable for the printer in terms of security. If the print data is determined to be printable ..., the print data is acquired from the selected storage ... print data stored in a storage cannot be transmitted to a printer if the storage and the printer have different security levels and when the security level of the printer is lower than that of the storage"*).

Furthermore, the above measures are taken in D6 for exactly the same purpose as in the present invention (see e.g. paragraphs [0168] and [0169]: *"This prevents the stored print data of the storage from being erroneously outputted from a printer whose security level is lower than that of the print data, thereby ensuring security for the print data ..., the print data stored in a storage is prevented from being transmitted to a printer when the security levels of the storage and printer do not match ..."*).

The board also notes that the skilled person would encounter no technical difficulties in applying the comparison of different security levels, which are already determined and stored in the system of D6, to the printer system of D1. Thus, the skilled person would arrive at the solution as claimed in an obvious manner, having regard to the combined teaching of D1

and D6.

3.2 In view of the above, the main request is not considered allowable under Article 56 EPC.

4. AUXILIARY REQUESTS

Claim 1 of the present auxiliary requests differs from claim 1 of the main request essentially in that it further specifies that (emphasis added)

I) the authentication information input means and the authentication means are part of the printer apparatus (**first to fourth auxiliary requests**);

J) the printer apparatus storage means is configured to record printer apparatus management information for each of the plurality of printer apparatuses having security attributes of each of the printer apparatuses including a security level and the printing system is configured to restrict printing the data on a printer apparatus identified by the print data restricting means when the security attributes for the print data has a security level higher than the security attributes of a printer apparatus among the printer apparatuses (**second to fourth auxiliary requests**);

K) the print data restricting means comprises data erasing means for erasing print data that has not been a target of a print instruction for at least a predetermined period and the printer apparatus attribute storage means stores a print history information for an indication that the data erasing means carried out erasing the print data (**second to fourth auxiliary requests**);

L) the printing system comprises an input portion for receiving print instructions from a user and that

the print attribute setting means receives from the user input security attributes for the print data for instructing formation of the print data from the user (**fourth auxiliary request**).

4.1 *Inventive step (Article 56 EPC)*

4.1.1 The feature analysis and reasoning outlined in point 3.1 above apply *mutatis mutandis* to claim 1 of the present auxiliary requests.

4.1.2 As to new feature I), the board notes that D1 palpably discloses that "authentication section 2" and "input section 4a", which perform the steps of features C) and D), are part of printer 1 (see e.g. D1, Figs. 2 and 3).

4.1.3 As to added feature J), it is apparent to the board that D6 also relies on a list comprising the security levels of the attached printers ("printer information storing section"; see e.g. D6, Fig. 3(b)) and that the data to be printed is not transmitted to the corresponding printer if the security level of the printer is lower than that for the data to be printed (see e.g. D6, paragraph [0167]), i.e. if the security level of the print data has a security level higher than the security level of that printer. Thus, feature J) is also disclosed in D6.

4.1.4 As to added feature K), the board holds that it solves the problem of avoiding the storage of unnecessary print data. This problem however is considered to be entirely unrelated to and thus independent of the objective problem solved on the basis of distinguishing feature H) (see point 3.1.2 above).

In addition, the deletion of data to be printed upon

expiry of a predetermined time period is a well-known measure in the field of printer network systems. This is, for example, demonstrated in document **D7** (see e.g. paragraph [0183], second sentence: *"A 'time-out' function may be included within the server function to automatically erase the print data of a print job from the storage function and to instruct the printers to delete that print job from their administration systems, after a predetermined time interval since the time of arrival of the print file in the system"*).

4.1.5 As to added feature L), the board notes that both D1 (see e.g. paragraph [0119] with regard to the user's setting of "confidential image data" or "secret data") and D6 (see e.g. paragraph [0158] as regards a user's "desired security level") demonstrate that a user's print instructions, including security attributes for the print data, are received and processed in the underlying printing systems, in accordance with feature L).

4.1.6 As a consequence, the subject-matter of claim 1 of the present auxiliary requests is likewise not considered to involve an inventive step, having regard to the teachings of D1, D6 and/or D7.

4.2 In conclusion, the first to fourth auxiliary requests on file are not allowable under Article 56 EPC either.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated